

1/20

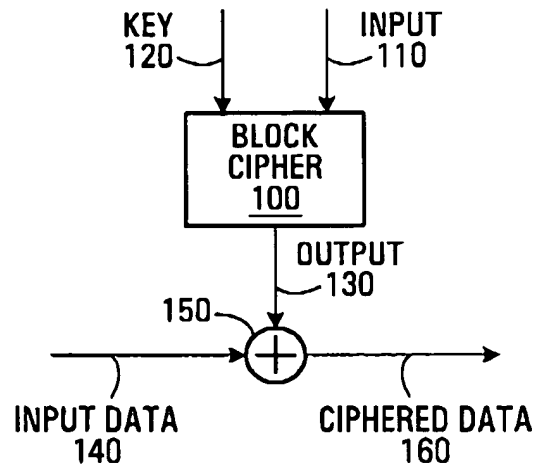


FIG. 1
(PRIOR ART)

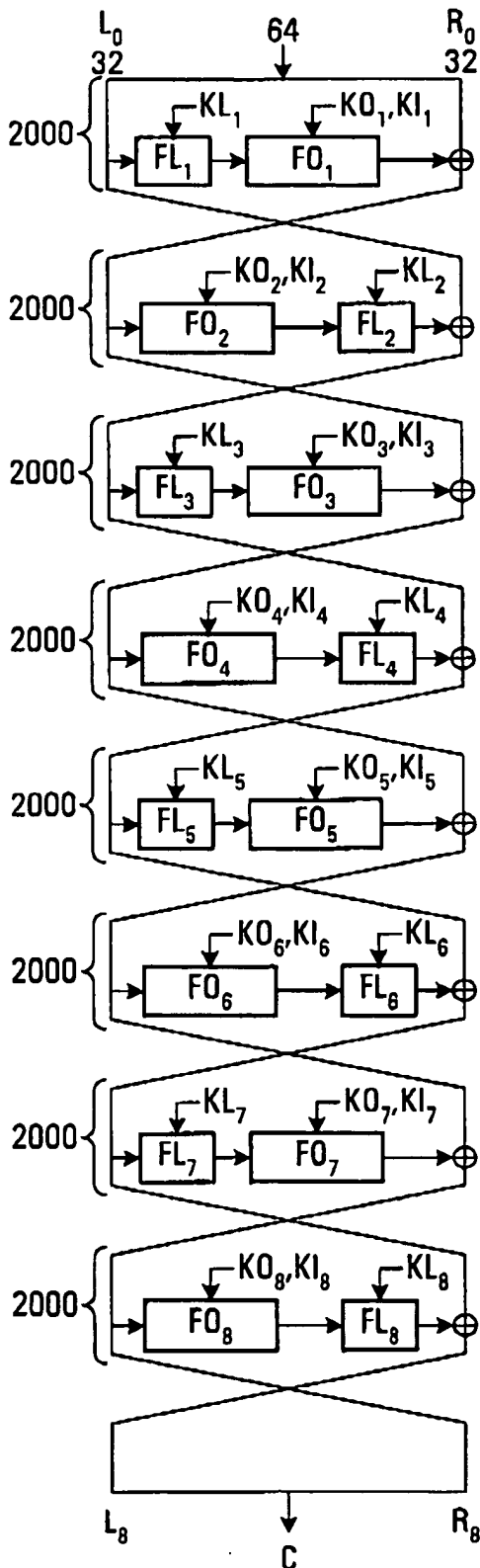


FIG. 2A
(PRIOR ART)

2/20

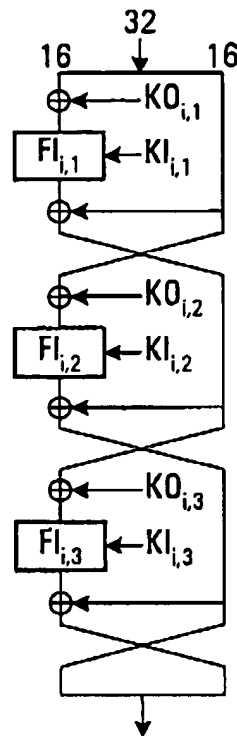


FIG. 2B
(PRIOR ART)

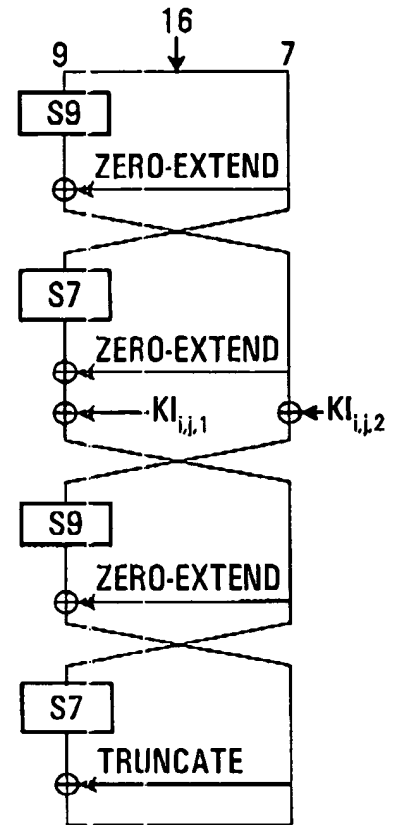


FIG. 2C
(PRIOR ART)

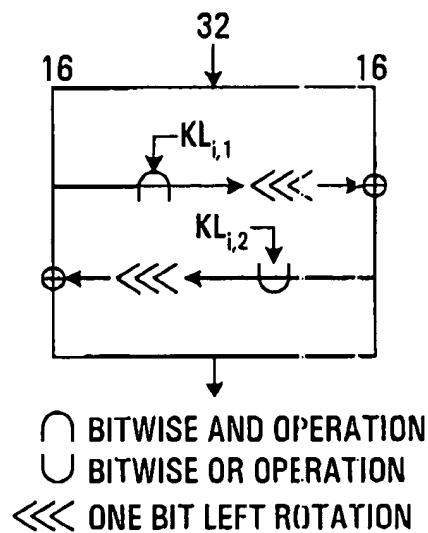


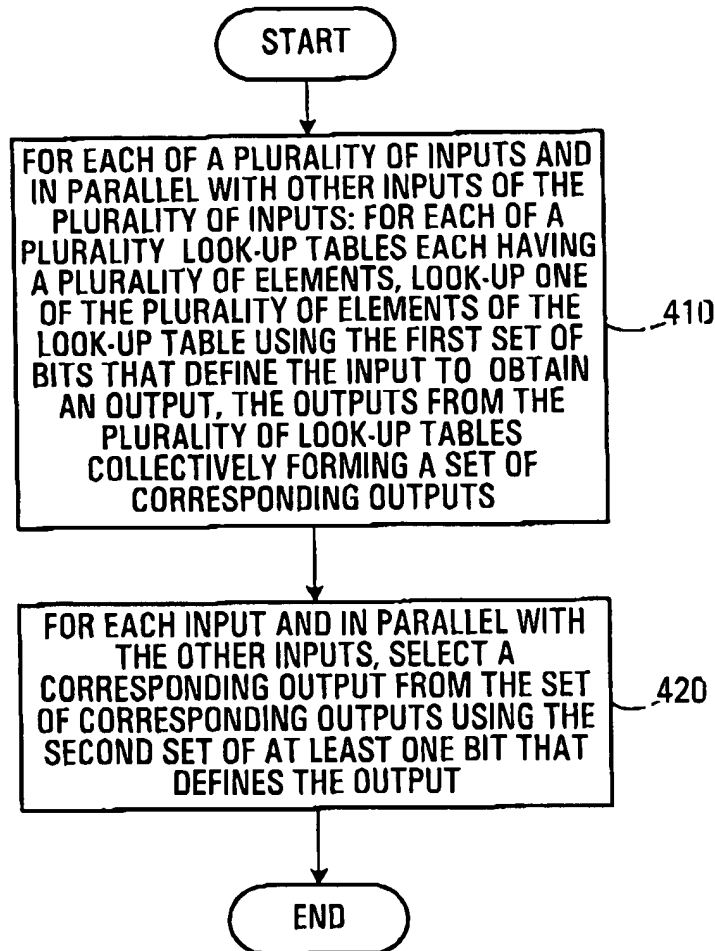
FIG. 2D
(PRIOR ART)

3/20

$$\begin{aligned}
200 &\longrightarrow Y_0 = x_1x_3 \oplus x_4 \oplus x_0x_1x_4 \oplus x_5 \oplus x_2x_5 \oplus x_3x_4x_5 \oplus x_6 \oplus x_0x_6 \oplus x_1x_6 \oplus x_3x_6 \oplus x_2x_4x_6 \oplus x_1x_5x_6 \oplus x_4x_5x_6 \\
201 &\longrightarrow Y_1 = x_0x_1 \oplus x_0x_4 \oplus x_2x_4 \oplus x_5 \oplus x_1x_2x_5 \oplus x_0x_3x_5 \oplus x_6 \oplus x_0x_2x_6 \oplus x_3x_6 \oplus x_4x_5x_6 \oplus 1 \\
202 &\longrightarrow Y_2 = x_0 \oplus x_0x_3 \oplus x_2x_3 \oplus x_1x_2x_4 \oplus x_0x_3x_4 \oplus x_1x_5 \oplus x_0x_2x_5 \oplus x_0x_6 \oplus x_1x_6 \oplus x_2x_6 \oplus x_4x_6 \oplus 1 \\
203 &\longrightarrow Y_3 = x_1 \oplus x_0x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_0x_5 \oplus x_0x_1x_5 \oplus x_2x_3x_5 \oplus x_1x_4x_5 \oplus x_2x_6 \oplus x_1x_3x_6 \\
204 &\longrightarrow Y_4 = x_0x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_4 \oplus x_0x_1x_4 \oplus x_2x_3x_4 \oplus x_0x_5 \oplus x_1x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_6 \oplus x_0x_3x_6 \oplus x_5x_6 \oplus 1 \\
205 &\longrightarrow Y_5 = x_2 \oplus x_0x_2 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_5 \oplus x_2x_5 \oplus x_4x_5 \oplus x_1x_6 \oplus x_1x_2x_6 \oplus x_0x_3x_6 \oplus x_3x_4x_6 \oplus x_2x_5x_6 \oplus 1 \\
206 &\longrightarrow Y_6 = x_1x_2 \oplus x_0x_3 \oplus x_0x_4 \oplus x_1x_5 \oplus x_3x_5 \oplus x_0x_1x_6 \oplus x_0x_2x_3x_6 \oplus x_1x_4x_6 \oplus x_0x_5x_6
\end{aligned}$$

FIG. 3
(PRIOR ART)

5/20

**FIG. 5**

6/20

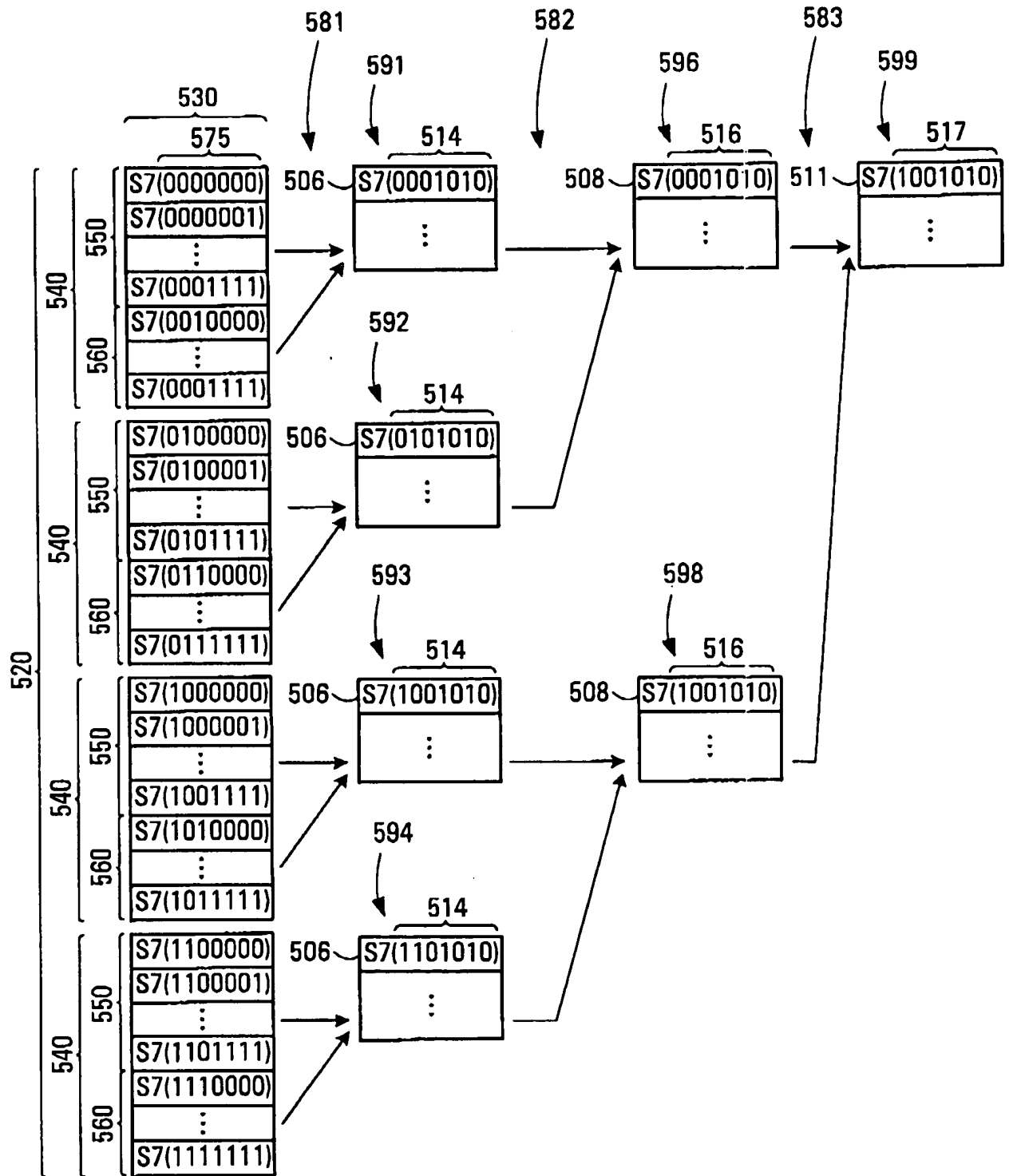


FIG. 6

7/20

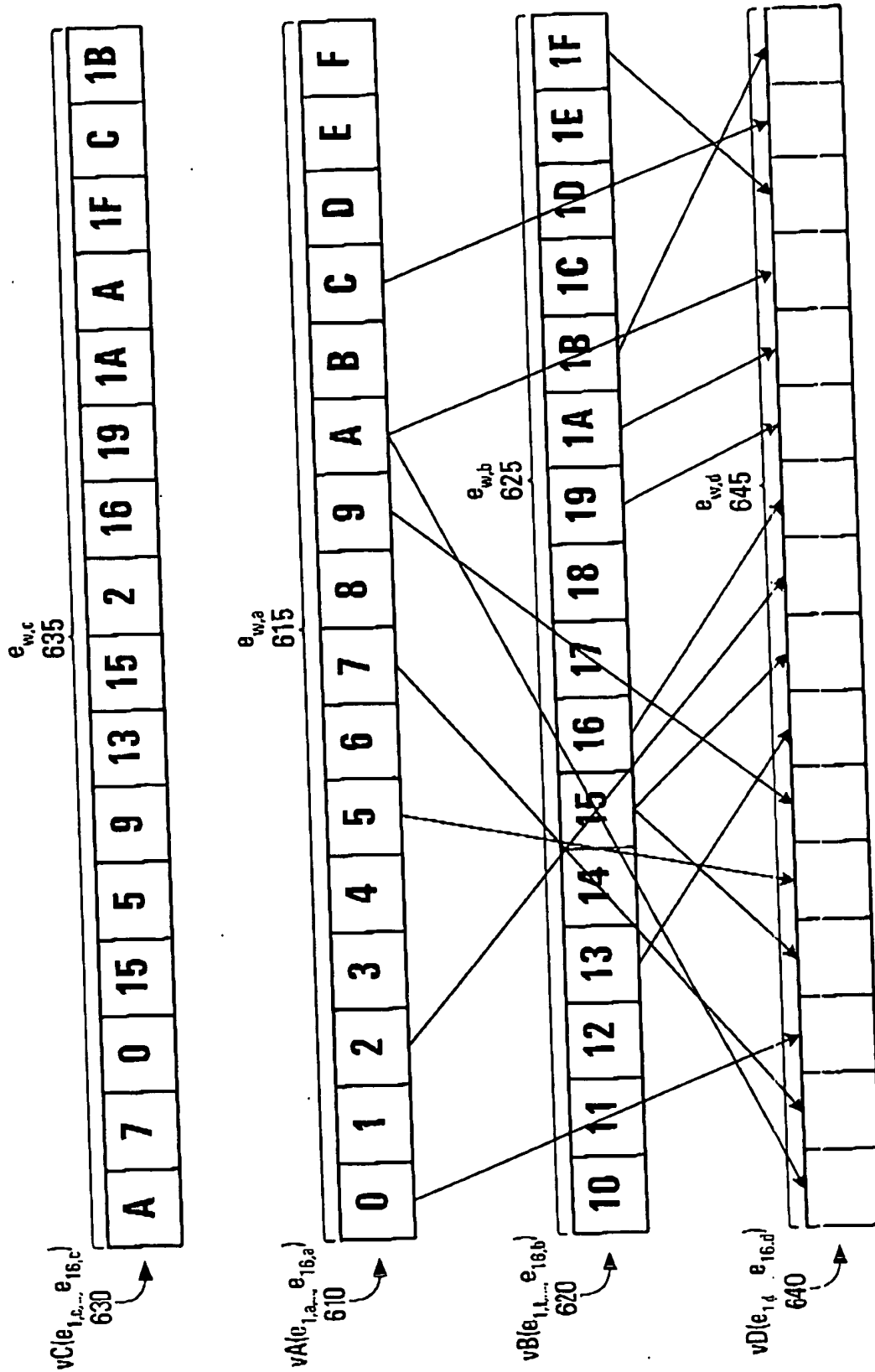
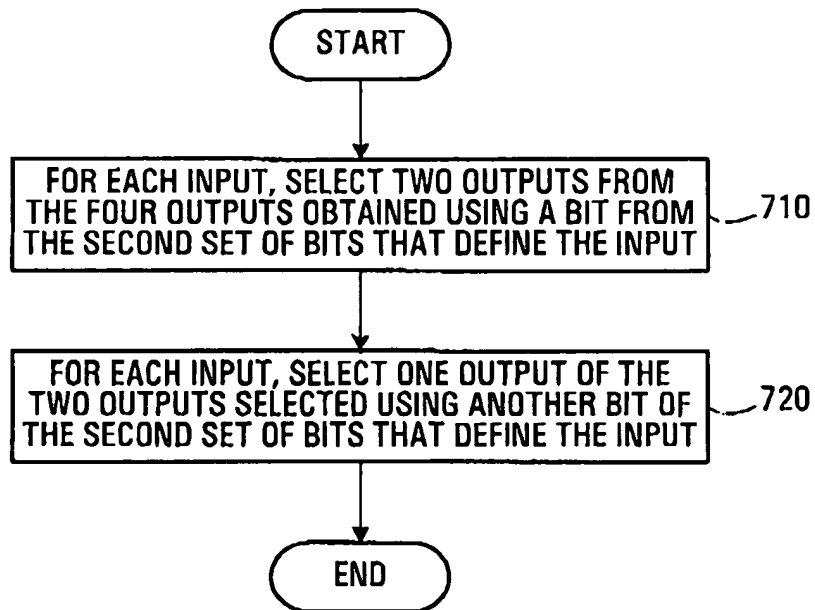
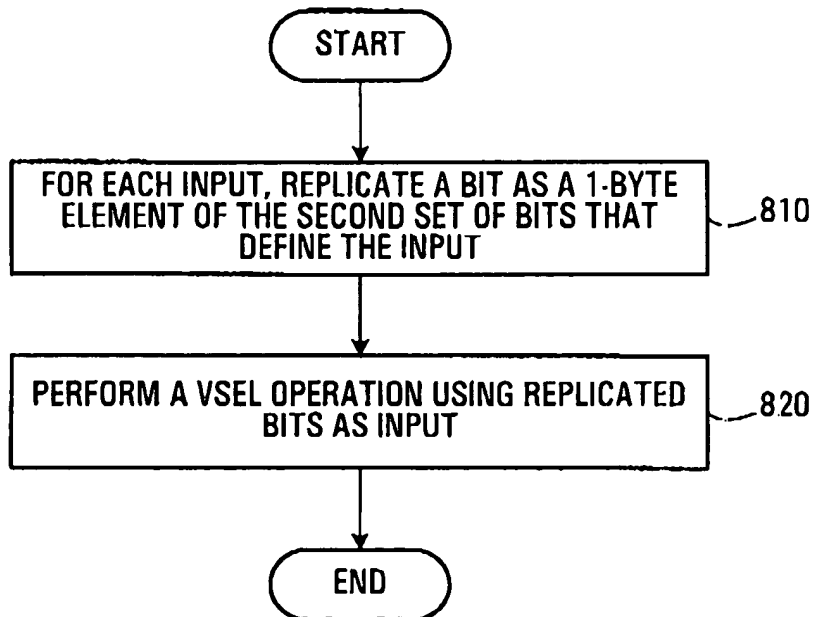


FIG. 7

8/20

**FIG. 8****FIG. 9**

+

9/20

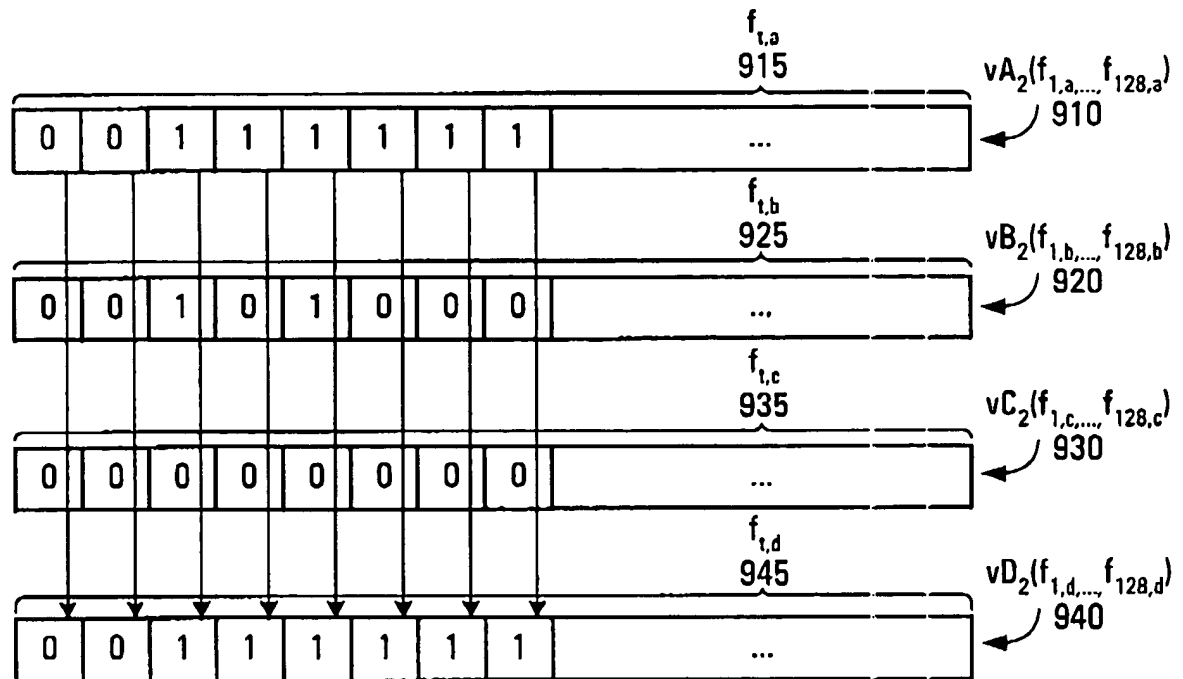


FIG. 10

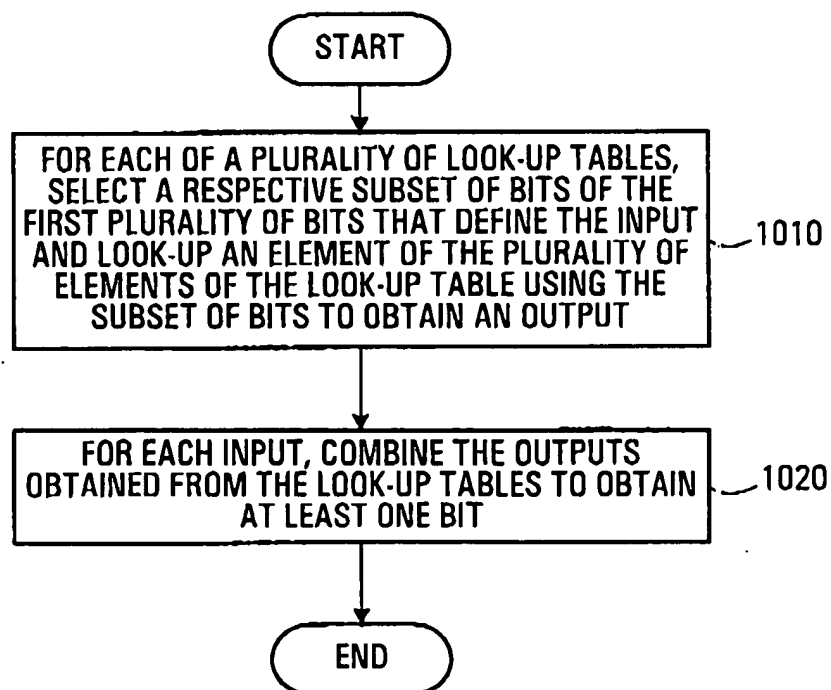


FIG. 11

+

10/20

1158	1157	1156	1155	1154	1153	1152	1151	1150	
Y_8	Y_7	Y_6	Y_5	Y_4	Y_3	Y_2	Y_1	Y_0	
$X'_2 X'_5$		$X'_2 X'_5$			$X'_2 X'_4$		$X'_3 X'_5$	$X'_4 X'_5$	1110 GROUP 1
								X'_3	
$X'_1 X'_5$		$X'_1 X'_5$	$X'_1 X'_4$	$X'_0 X'_5$		$X'_0 X'_5$	$X'_0 X'_4$		1120 GROUP 2
							$X'_0 X'_5$		
							$X'_1 X'_4$		
$X'_1 X'_6$			$X'_0 X'_6$	$X'_0 X'_7$	$X'_0 X'_6$		$X'_1 X'_7$	$X'_0 X'_2$	1130 GROUP 3
X'_7			$X'_1 X'_6$		$X'_1 X'_6$			$X'_0 X'_7$	
								$X'_1 X'_7$	
								$X'_2 X'_7$	
$X'_3 X'_4$	$X'_2 X'_6$	$X'_3 X'_6$	$X'_3 X'_7$	$X'_3 X'_6$		$X'_2 X'_6$	$X'_2 X'_3$		1140 GROUP 4
$X'_6 X'_4$	$X'_2 X'_7$					$X'_3 X'_4$	$X'_2 X'_7$		
	X'_3					$X'_3 X'_8$			
	$X'_3 X'_6$								
$X'_0 X'_1$	$X'_0 X'_1$	X'_0	X'_2	$X'_0 X'_1$	X'_0				1150 GROUP 5
$X'_1 X'_2$	$X'_0 X'_2$	$X'_1 X'_8$		$X'_1 X'_3$	$X'_0 X'_3$	$X'_0 X'_3$	$X'_0 X'_1$		
X'_2	$X'_0 X'_3$	$X'_2 X'_3$		$X'_1 X'_8$	$X'_0 X'_8$	$X'_0 X'_8$	X'_1		
$X'_2 X'_8$	$X'_1 X'_2$	$X'_3 X'_8$		$X'_2 X'_8$	$X'_1 X'_2$	X'_1			
$X'_3 X'_8$	$X'_2 X'_3$			$X'_3 X'_8$	$X'_1 X'_8$				
	$X'_4 X'_5$	$X'_5 X'_4$	$X'_5 X'_4$	X'_4	$X'_4 X'_7$	$X'_5 X'_6$	$X'_5 X'_8$	$X'_4 X'_8$	1160 GROUP 6
	$X'_5 X'_7$	$X'_5 X'_6$	$X'_5 X'_8$	$X'_6 X'_7$	X'_5	$X'_5 X'_7$	X'_6	$X'_5 X'_6$	
	X'_8	$X'_5 X'_8$	$X'_6 X'_7$		$X'_7 X'_8$	$X'_6 X'_7$	"1"	$X'_5 X'_8$	
	"1"	$X'_6 X'_4$	$X'_6 X'_8$			$X'_7 X'_4$		$X'_7 X'_8$	
		X'_7	$X'_7 X'_4$			X'_8		"1"	
		$X'_7 X'_8$	$X'_7 X'_8$			"1"			
			"1"						

FIG. 12

11/20

1200

GROUP NUMBER	1210								1220								1230								1240	1250
	y'_8	y'_7	y'_6	y'_5	y'_4	y'_3	y'_2	y'_1	y'_0	NUMBER OF BITS GENERATED THAT DEPEND DEPENDENT ON x'_p	x'_8	x'_7	x'_6	x'_5	x'_4	x'_3	x'_2	x'_1	x'_0	NUMBER OF BITS USED FOR LOOKING UP TABLE	NUMBER OF VECTORS A VPERM INSTRUCTION OPERATES ON					
1	✓		✓	X	X	✓	X	✓	✓	5			✓	✓			✓				4	1				
2	✓		✓	✓	✓	X	✓	✓	X	7				✓	✓			✓		✓	4	1				
3	✓		X	✓	✓	✓	X	✓	✓	6			✓				✓			✓	5	2				
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	7			✓	✓			✓				5	2				
5	✓	✓	✓	✓	✓	✓	✓	✓	✓	8							✓			✓	5	2				
6		✓	✓	✓	✓	✓	✓	✓	✓	8			✓	✓	✓						5	2				

1260

1270

1280

FIG. 13

12/20

1300

1310

1320

1340

GROUP NUMBER	BIT ORDERING AS AN INPUT		RE-ORDERED BITS	INSTRUCTION
1	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$x'_7 x'_6 \overset{1330}{\boxed{x'_5 x'_4 x'_3 x'_2}}$	vsrb
2	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$x'_7 x'_6 \overset{1331}{\boxed{x'_5 x'_4 x'_1 x'_0}}$	vsel
3	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$x'_5 x'_4 x'_3 \overset{1332}{\boxed{x'_2 x'_1 x'_0 x'_7 x'_6}}$	vrlb
4	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$x'_7 x'_6 x'_5 \overset{1333}{\boxed{x'_4 x'_3 x'_2 x'_7 x'_6}}$	vsel
5	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$x'_8 x'_5 x'_4 \overset{1334}{\boxed{x'_3 x'_2 x'_1 x'_0 x'_8}}$	vslb & vsel
6	$x'_8 x'_7 x'_6 x'_5 x'_4 x'_3 x'_2 x'_1 x'_0$	→	$\overset{1335}{\boxed{x'_7 x'_6 x'_5 x'_4 x'_8}}$	vsrb & vsel

FIG. 14

+

13/20

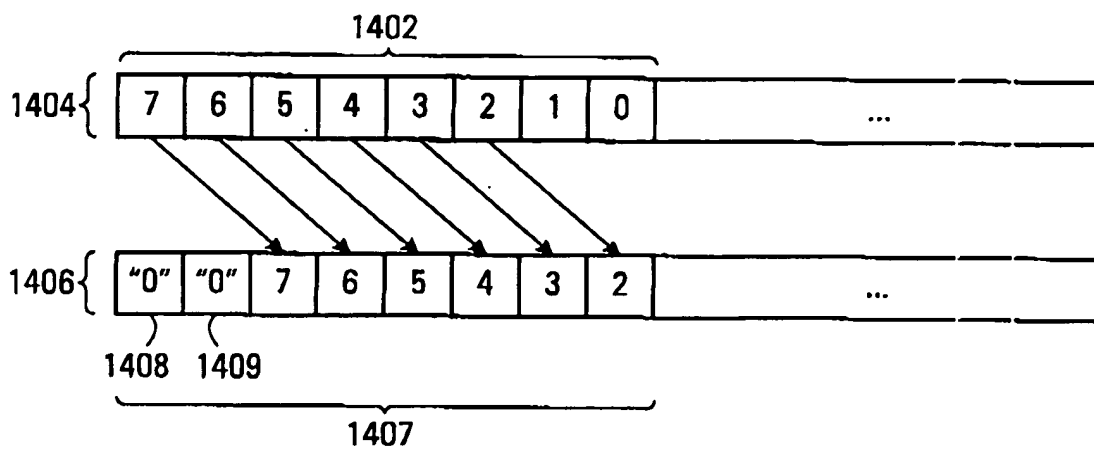


FIG. 15A

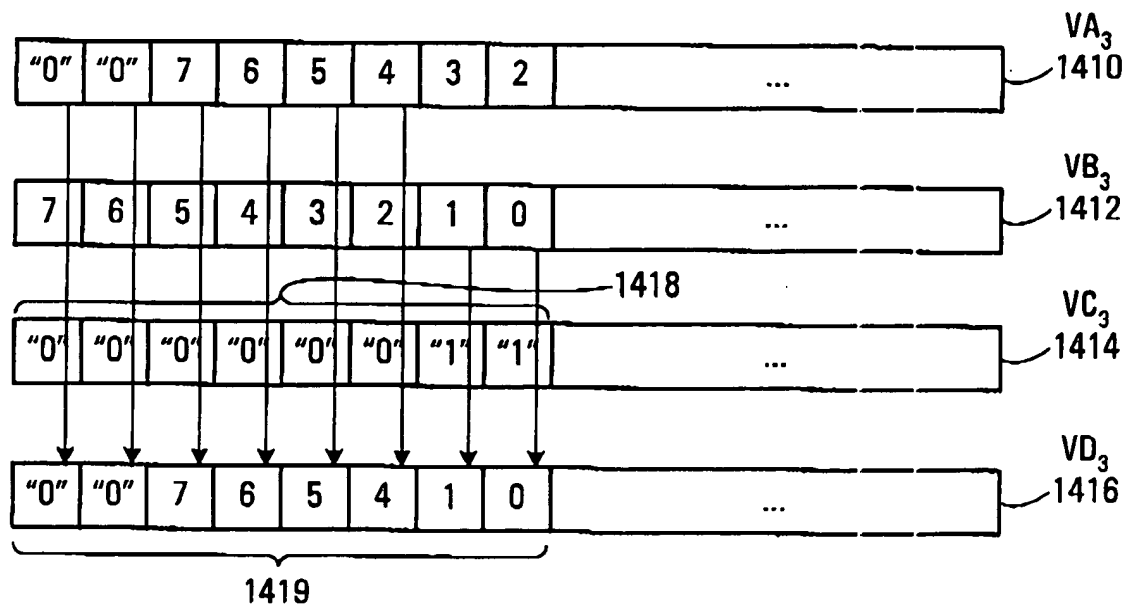


FIG. 15B

+

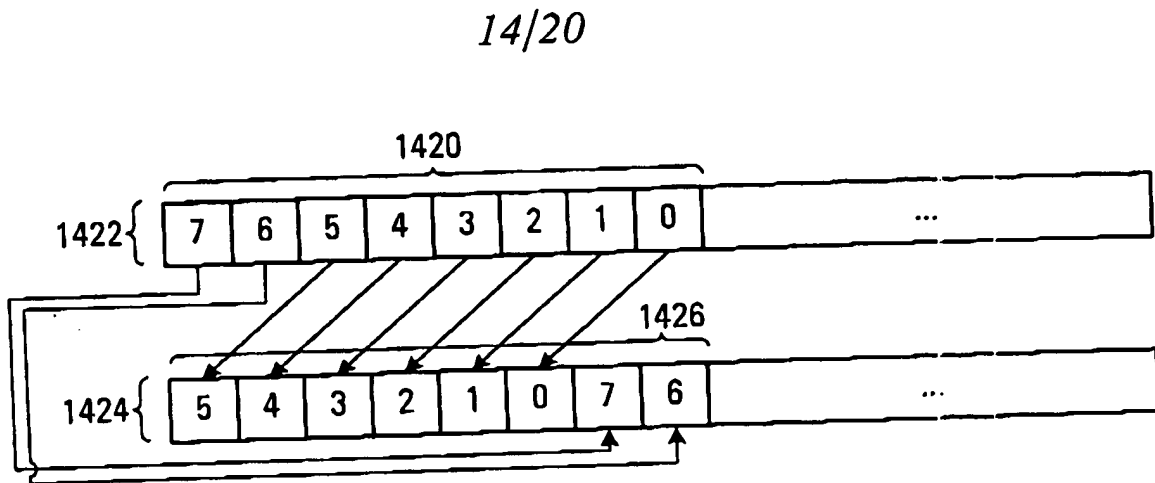


FIG. 15C

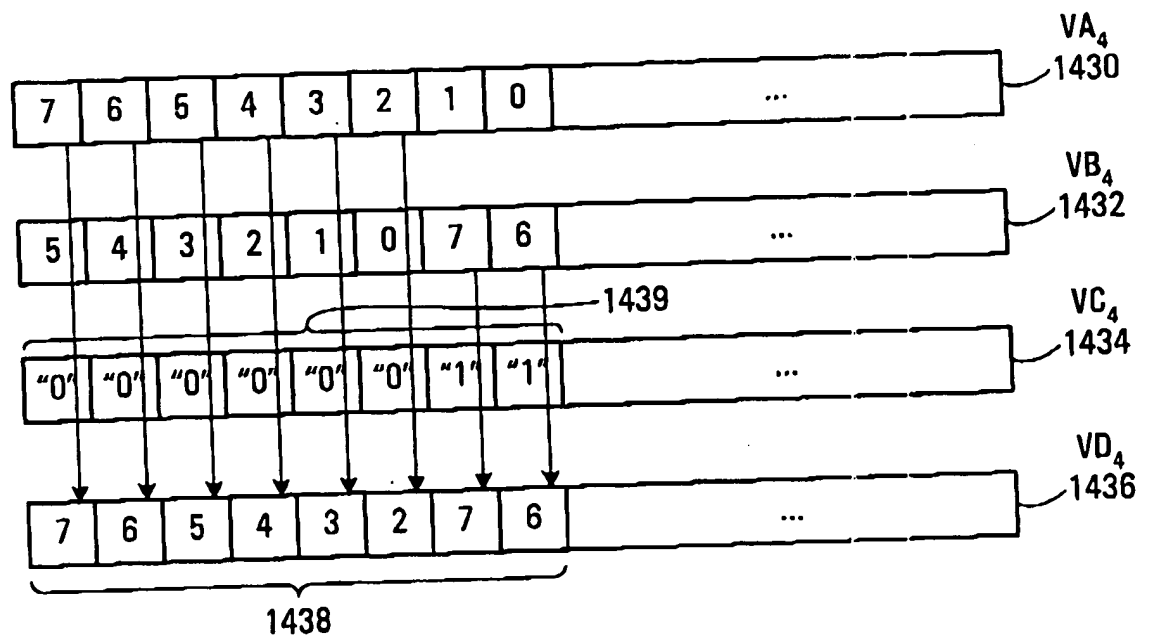


FIG. 15D

15/20

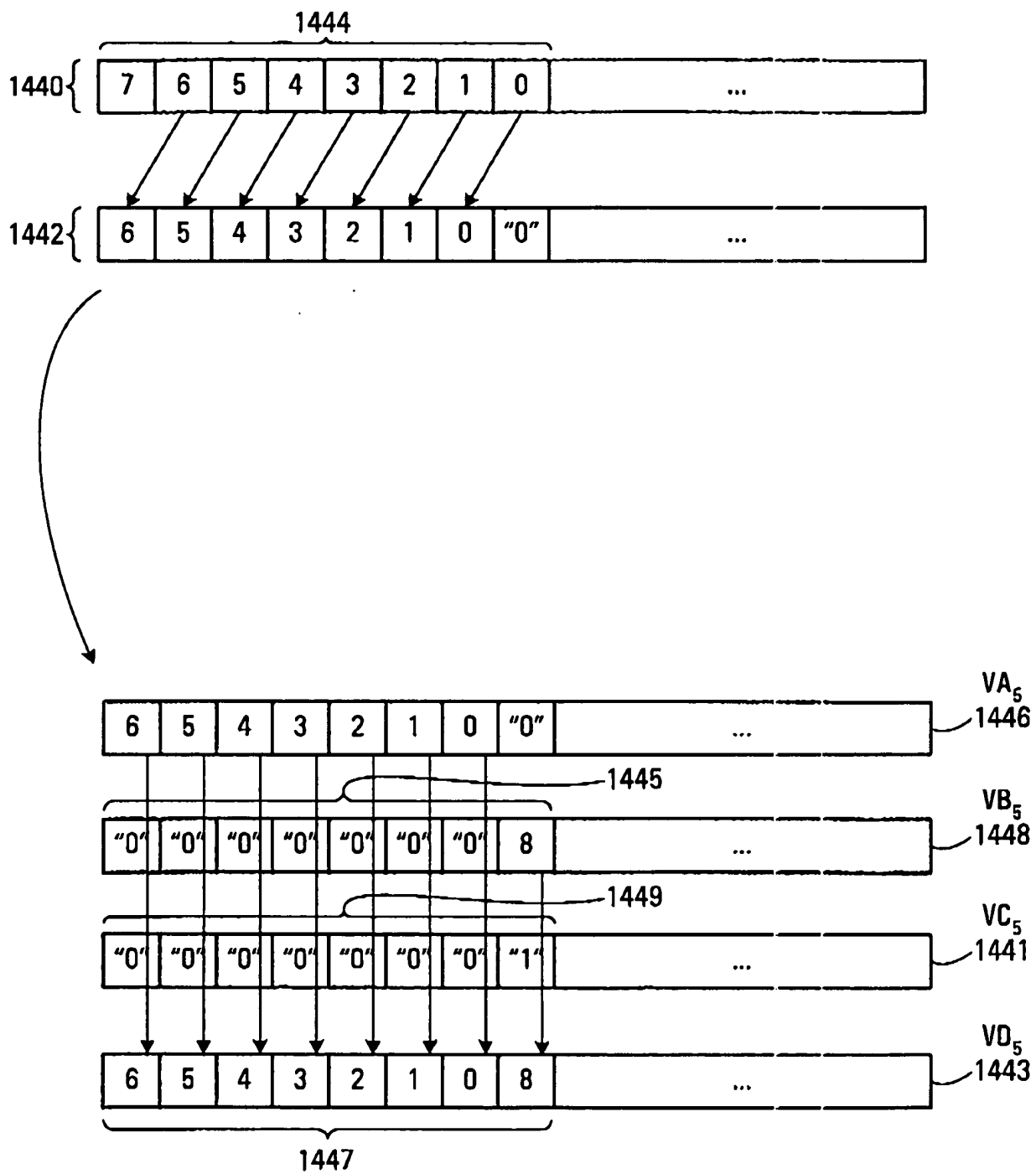


FIG. 15E

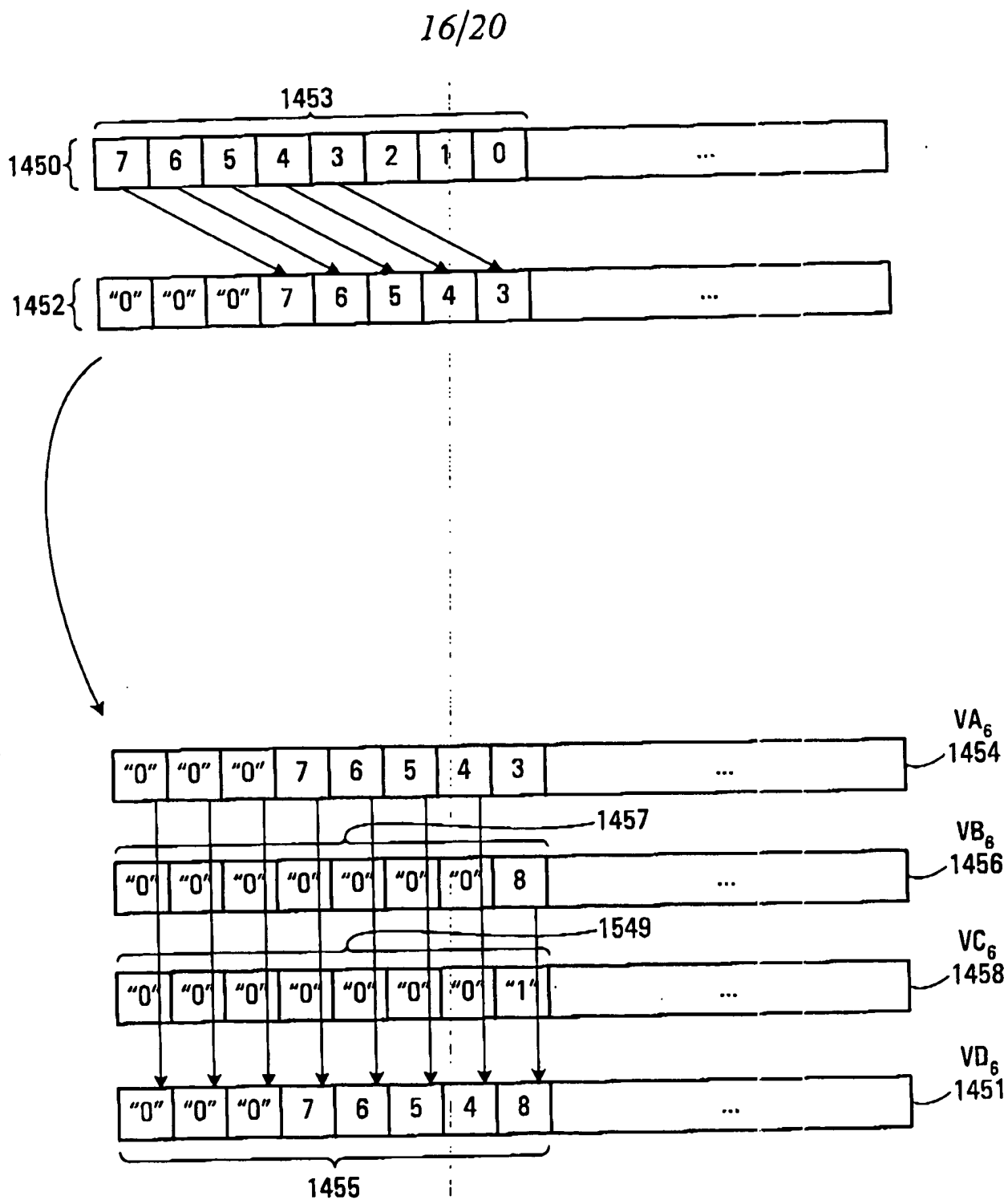
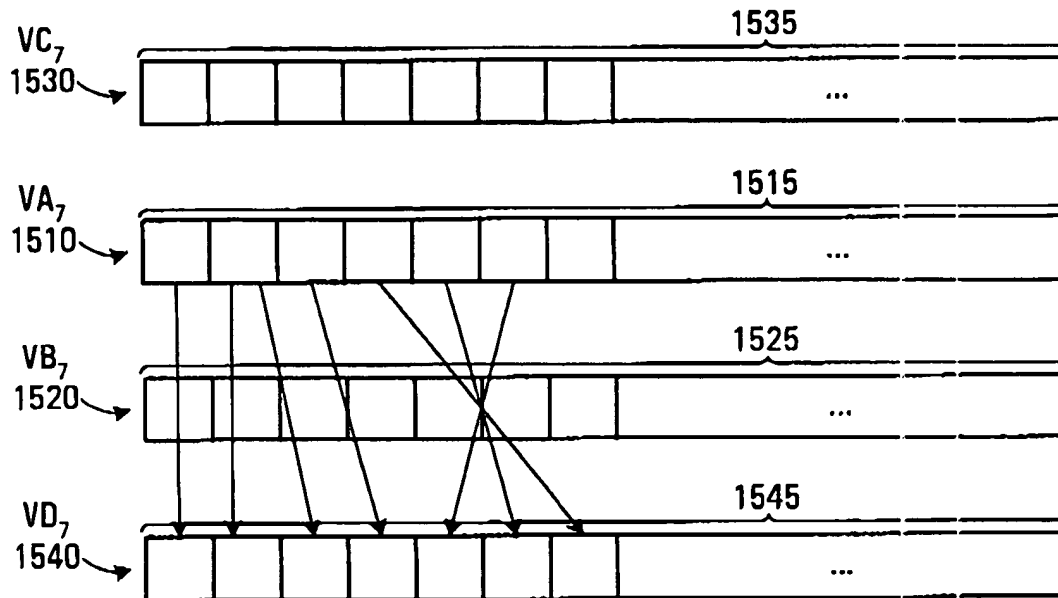
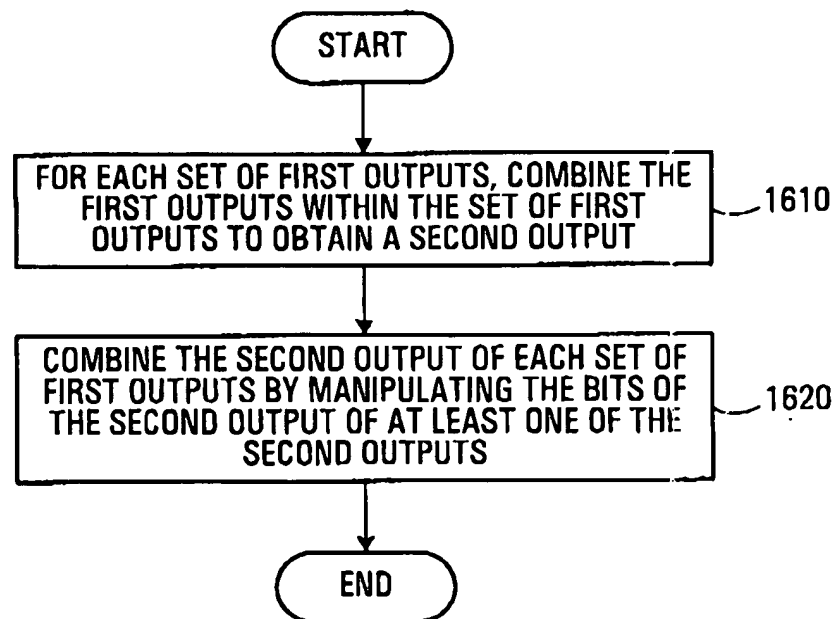


FIG. 15F

17/20

**FIG. 16****FIG. 17**

18/20

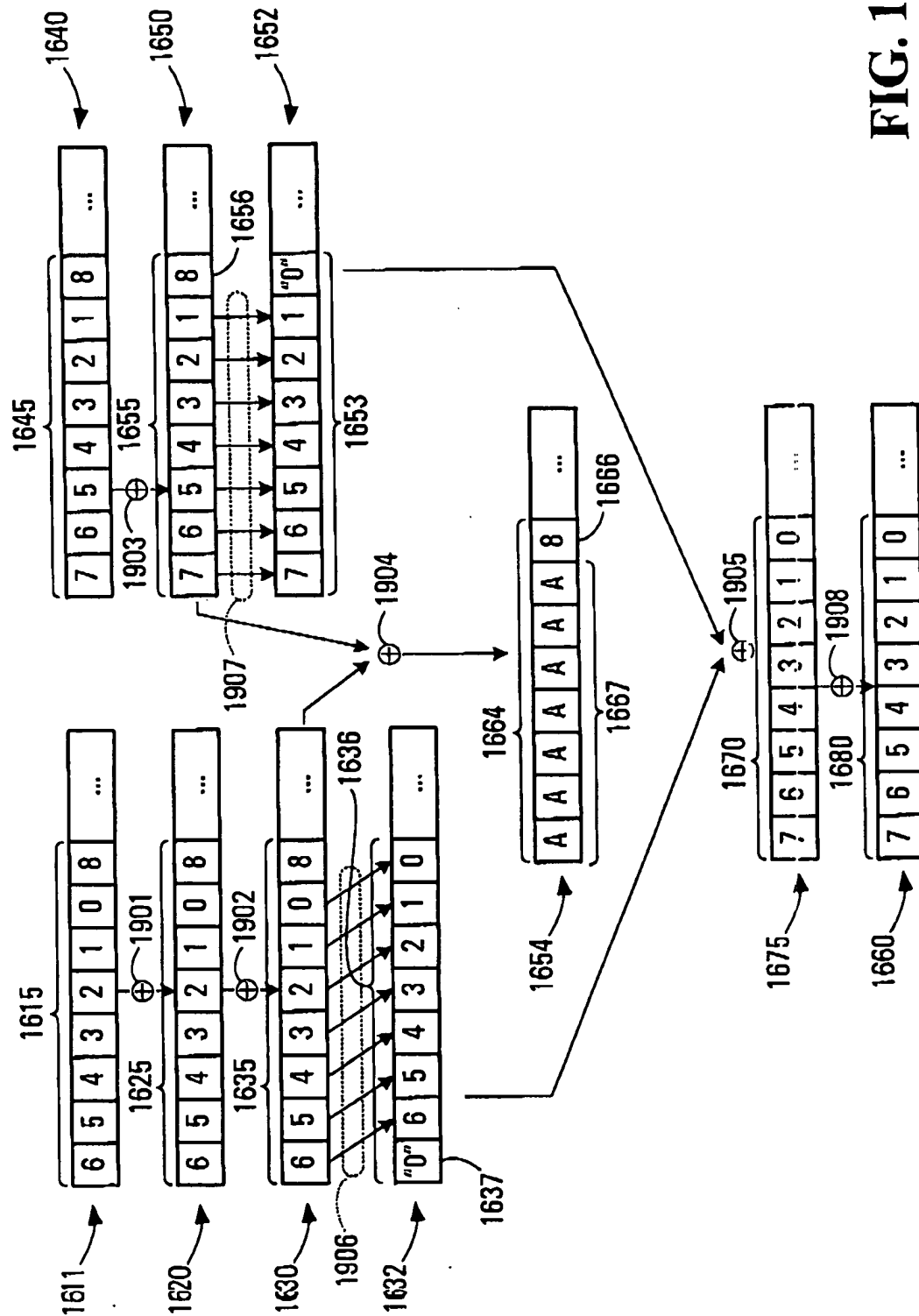
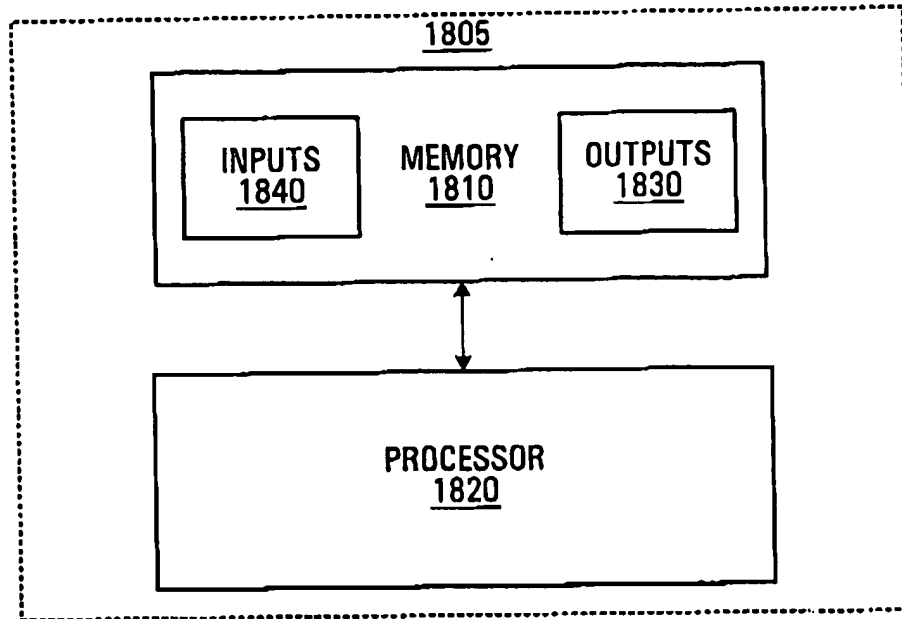
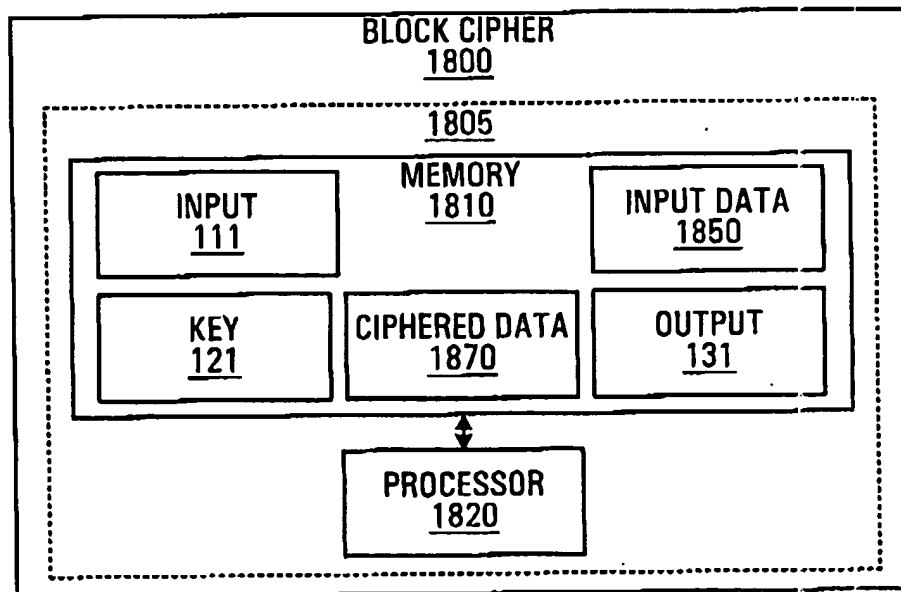


FIG. 18

19/20

**FIG. 19A****FIG. 19B**

20/20

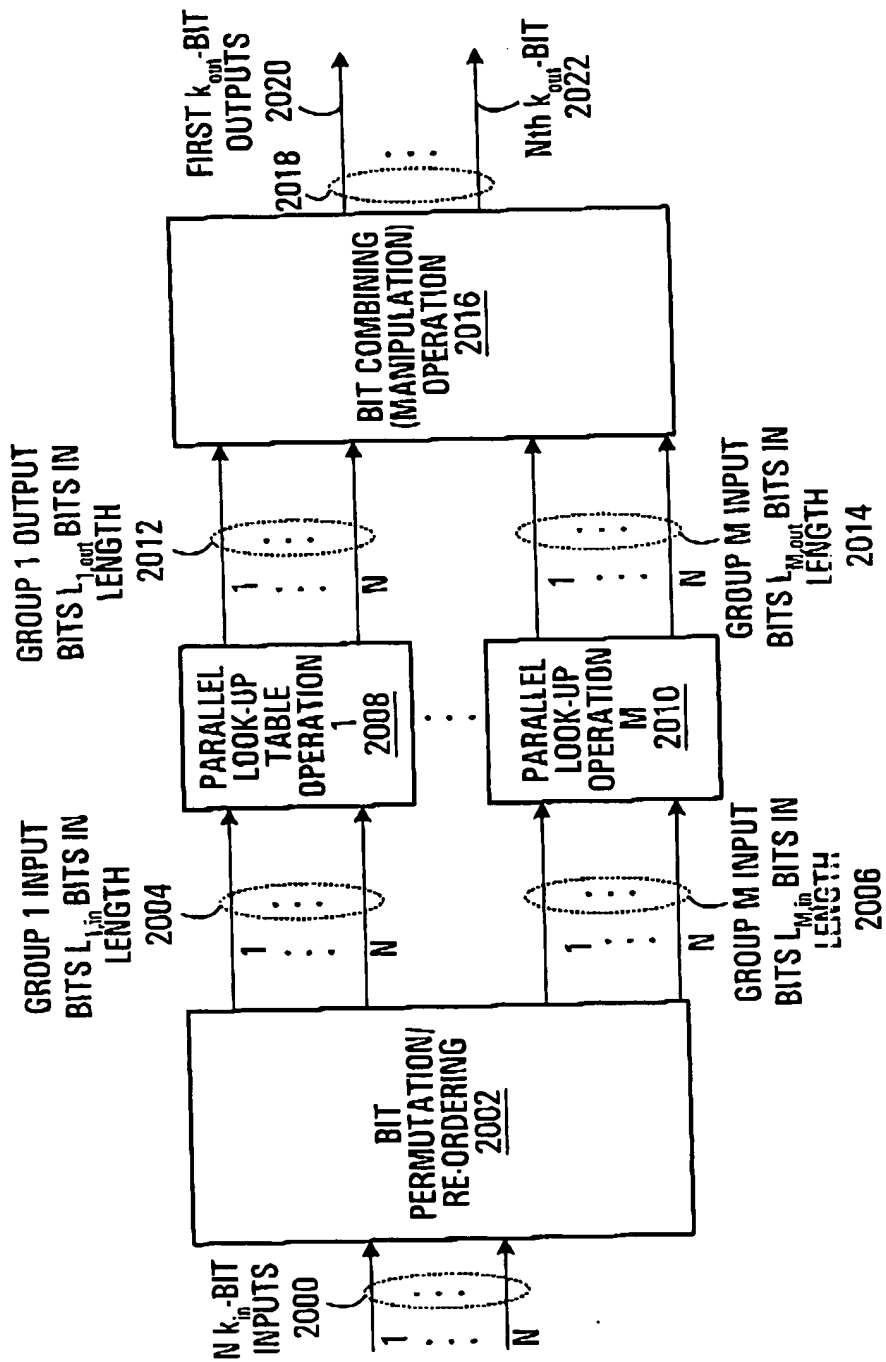


FIG. 20